

--ABSTRACT

The invention concerns a method for verifying a signature or an authentication between a prover and a verifier based on an asymmetric cryptographic calculation algorithm. The prover calculates (1) at least one prevalidation value q , which is a quotient of two cryptographic values a , b by the public modulo n , and transmits this value q to the verifier. The verifier calculates (3) the products $a*b$ and $q*n$ and the difference $a*b-q*n$ in order to perform at least one modular reduction without a division operation. The invention applies to signature or authentication verification between a proving microcomputer and a verifying microprocessor card.--

3 the equality of said difference and the validity of said authentication without any division
4 operation for the modular reduction.

1 12. Method according to claim 1, characterized in that said response value, the
2 encrypted value B, and said quotient value Q are concatenated prior to their transmission
3 from the prover entity to the verifier entity.

1 13. Utilization of the method according to claim 1, the verifier entity
2 comprising an embedded system such as a microprocessor card and the prover entity
3 comprising an embedded card reading system.

Sub
A7

5

prevalidation

10

P